CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会活動報告

2025年7月25日

暗号技術検討会 座長
産業技術総合研究所 フェロー
横浜国立大学 上席特別教授
松本 勉

目次

1.CRYPTRECの概要

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECとは

CRYPTography **R**esearch and **E**valuation **C**ommittees

CRYPTRECの概要

■ デジタル庁・総務省・経済産業省・NICT・IPAが共同で開催する暗号技術評価プロジェクト

■ 当プロジェクトは、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討すること等を通じて、セキュアなIT社会の実現を目指すもの

■ 暗号技術検討会並びに暗号技術検討会の下に設置される暗号技術評価委員会及び暗号技術活用委員会により運営

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC活動体制（2024年度）

暗号技術検討会 （事務局：デジタル庁、総務省、経済産業省）

① CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
② CRYPTREC暗号リストの改定に関する調査・検討
③ 関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

暗号技術評価委員会 （事務局：NICT、IPA）

① 暗号技術の安全性及び実装に係る監視及び評価
② 新世代暗号に係る調査
③ 暗号技術の安全な利用方法に関する調査

暗号技術調査WG
（耐量子計算機暗号）
（2021年7月～ ）

暗号技術活用委員会 （事務局：IPA、NICT）

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
② 暗号技術の利用状況に係る調査及び必要な対策の検討
③ 暗号政策の中長期的視点からの取組の検討

暗号鍵管理
ガイダンスWG
（2021年6月～ ）

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会構成員

座長	松本 勉	国立研究開発法人産業技術総合研究所 フェロー 横浜国立大学 先端科学高等研究院 上席特別教授
構成員	阿部 正幸	日本電信電話株式会社 フェロー
	石井 義則	一般社団法人情報通信ネットワーク産業協会 常務理事
	上原 哲太郎	立命館大学 教授
	國廣 昇	筑波大学 教授
	黒田 真弓	一般社団法人テレコムサービス協会 技術・サービス委員会 副委員長
	島岡 政基	セコム株式会社 IS研究所 主幹研究員
	高木 剛	東京大学 教授
	田村 裕子	日本銀行 金融研究所 企画役
	本間 尚文	東北大学 教授
	松井 充	三菱電機株式会社 研究開発本部　シニアフェロー
	松浦 幹太	東京大学 教授
	松本 泰	特定非営利活動法人日本ネットワークセキュリティ協会 フェロー
	吉田 博隆	国立研究開発法人産業技術総合研究所 研究チーム長
	渡邊 創	国立研究開発法人産業技術総合研究所 研究部門長

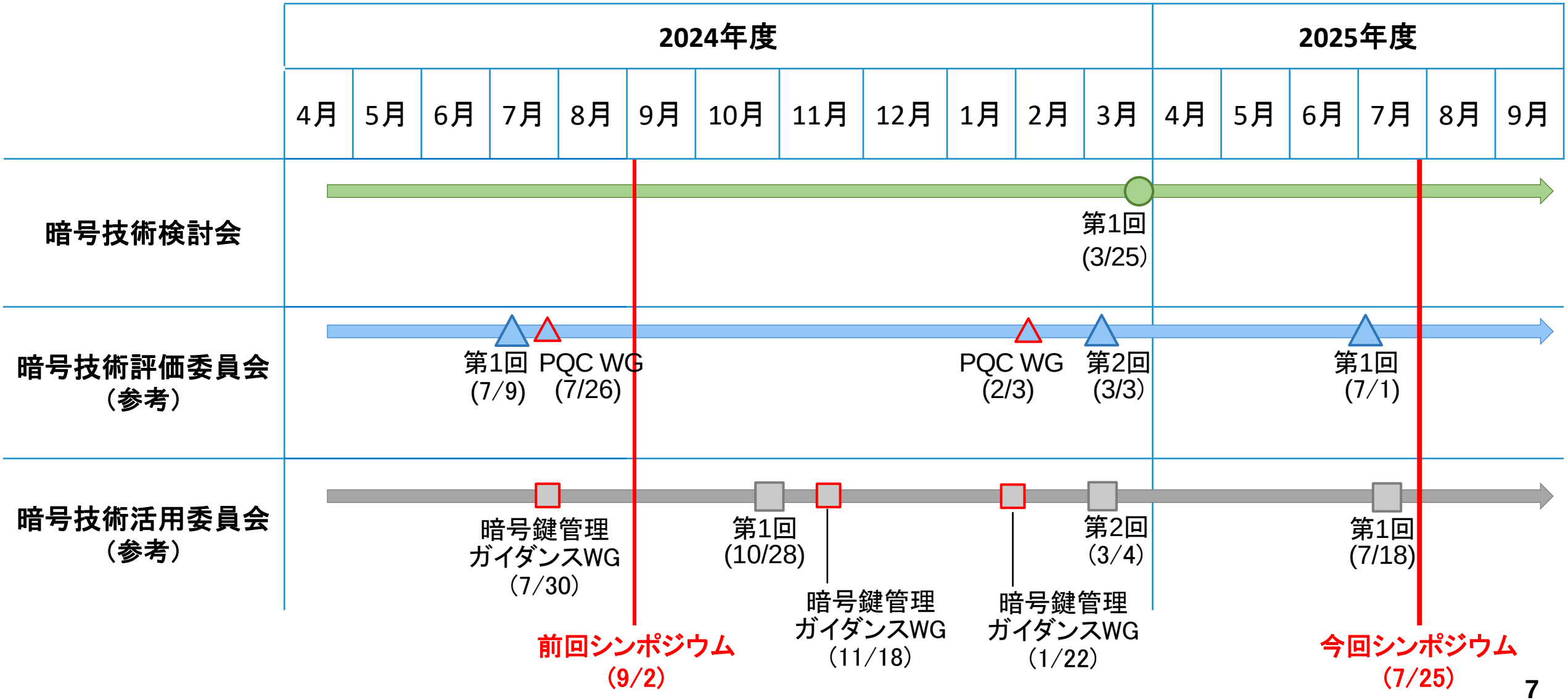
（五十音順、敬称略、所属は2025年6月時点のもの）

オブザーバ：内閣サイバーセキュリティセンター、警察庁、個人情報保護委員会、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、経済産業省、防衛省、NICT、AIST、IPA、JIPDEC、FISC

事務局：デジタル庁、総務省、経済産業省

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会等の開催状況



2.暗号技術検討会の活動概要

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの概要

- CRYPTRECの活動を通して**安全性・実装性能等が確認された暗号技術**について、デジタル庁、総務省及び経済産業省において**電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）**を策定。
- CRYPTREC暗号リストは以下の**3リスト**により構成される。（注：現在の3リスト構成は2013年より）

①電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、市場における利用実績が十分であるか今後の普及が見込まれ、利用を推奨するもののリスト

②推奨候補暗号リスト

安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト

③運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったと確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト移行ルール

次の条件のいずれかを満たすと暗号技術検討会が決定した場合
1. ５年ごとの利用実績調査により、複数の利用実績を確認した場合
2. その他、普及していることが明らか又は急速な普及が大いに見込まれる場合

①電子政府推奨暗号リスト

安全性維持が困難（危殆化した）と暗号技術検討会が決定した場合

※ 電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保する必要があるため、いきなりリストから削除することはしない。

標準化等により将来的な利用が見込まれ、安全性や実装性能が十分にあると暗号技術検討会が決定した場合（公募や事務局提案等）

②推奨候補暗号リスト

- CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかったもの
- 公募提案暗号について、提案会社より自主取下げ要望があり、暗号技術検討会における審議の結果「今後の普及が見込まれない公募提案暗号」であると判断されたもの

安全性維持が困難（危殆化した）と判断した場合

③運用監視暗号リスト

（2019年度暗号技術検討会　決定事項）

次の条件のいずれかを満たすと暗号技術検討会が決定した場合、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。

1. 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
2. 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
3. その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

リストから削除

※ 利用実績調査の具体的な実施内容・評価基準は、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドライン類の作成等（暗号技術評価委員会）

■ 耐量子計算機暗号ガイドライン（2024年度版）

- 量子コンピュータの実用化により一部の公開鍵暗号方式の安全性が低下することを踏まえ、耐量子計算機暗号に関する調査結果をまとめたもの。
- 「耐量子計算機暗号の研究動向調査報告書」と、調査報告書を簡略化した「耐量子計算機暗号ガイドライン」（それぞれ2022年度版）発行以降の研究技術動向に関して調査を行い、2024年度版を作成。
- 2022年度版とは異なり、耐量子計算機暗号の活用方法を調査報告書・ガイドラインの両方に記載。
- 対象：
  - ➢ 調査報告書：暗号技術に携わる研究者・技術者。 ➢ ガイドライン：一般的な読者・暗号初学者。

■ 外部評価「量子コンピュータが共通鍵暗号の安全性に及ぼす影響」

- 2019年度「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」（外部評価報告書）を更新する形で、2024年度の技術動向調査及び外部評価結果を反映し、2024年度版を作成。
- 2024年度外部評価報告書から、CRYPTREC電子政府推奨暗号リスト掲載の共通鍵暗号技術とNIST標準軽量暗号Asconの安全性に量子計算機が及ぼす影響は、汎用量子アルゴリズム（特に、Groverのアルゴリズムと BHTのアルゴリズム※）のみを考慮すれば十分であるという結論を得た。

※ Groverのアルゴリズムを応用し、nビットハッシュ関数の衝突探索を時間$O(2^{n/3})$で探索するアルゴリズム。

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドライン類の作成等（暗号技術活用委員会）

■ 暗号鍵管理ガイダンスの拡充

- 暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理の設計で明記する事項や考慮する点などを解説することを目的としたガイダンス。
- 2023年度に発行した「暗号鍵管理ガイダンス」において記載を見送った部分についてのガイダンスを作成。分冊構成としたため、2023年度のガイダンスを「暗号鍵管理ガイダンスPart1」、2024年度のガイダンスを「暗号鍵管理ガイダンスPart2」として位置付けた。
- 対象：暗号鍵管理機能を持つシステムの設計者。

■ 暗号利活用のための新たなガイダンスの検討

- 「クラウドにおける鍵管理」をテーマとする新たなガイダンスの作成方針を検討。クラウドを利用した情報システムにおける鍵管理の留意事項を解説することを目的とする。
- 本ガイダンスの策定にあたって、2025年度より新たなWGを設置予定（おおむね2年程度での完成を想定）。WG委員として、CSP事業者、SI事業者・SaaS事業者、クラウドHSMベンダ、クラウドサービス利用者、大学や関連団体などの有識者に参画いただく予定。
- 対象：クラウドサービスを利用した情報システムの構築者（SI事業者）、運用者、利用者。

CRYPTREC
Cryptography Research and Evaluation Committees

2025年度における耐量子計算機暗号関連の活動について

- CRYPTRECでは、2025年度も、電子政府推奨暗号等の安全性を評価・監視するとともに、暗号技術の更なる普及促進を行うべく検討を進める。

- 暗号技術検討会においては、**CRYPTREC暗号リストの更新等について必要に応じて検討を行う**予定である。

- 暗号技術評価委員会においては、NISTをはじめとする世界各国の機関において耐量子計算機暗号の選定・標準化活動が継続されており、**情勢が流動的であることに鑑み、引き続き暗号技術調査ワーキンググループ（耐量子計算機暗号）を設置して、耐量子計算機暗号に関する最新動向を把握する**とともに、**社会的動向を踏まえてNIST標準として公開されたFIPS-203,204,205について安全性評価・実装性能評価関連の活動を開始した**。

- 暗号技術活用委員会においては、**耐量子計算機暗号をめぐる社会的動向を踏まえ、耐量子計算機暗号の取扱い基準や位置づけ・記載内容等についての検討を開始した。**具体的には各国政府・公的機関等が公表している「PQCへの移行（方針）」の政策やガイドラインについて政策的側面からの整理、及び「CRYPTREC暗号リスト」上のPQCの位置づけや移行ルールを変更すべきかどうかを検討し、委員会としての見解を取りまとめる予定。

CRYPTREC Cryptography Research and Evaluation Committees

耐量子計算機暗号移行に関する最近の政府の動向

- **政府機関等におけるPQC利用**に関し、関係府省庁の緊密な連携のもと必要な施策を検討・推進するため、**内閣官房とりまとめのもと、「耐量子計算機暗号(PQC)利用に関する関係府省庁連絡会議」を2025年6月30日に設置**。
- 年内に工程表（ロードマップ）の骨子（移行の方向性）をとりまとめ、サイバーセキュリティ戦略の改定に反映される予定。

耐量子計算機暗号(PQC)利用に関する関係府省庁連絡会議

＜参加者＞

議長	内閣官房副長官補（内政担当）
副議長	内閣官房内閣審議官（国家安全保障局）
	内閣官房内閣審議官（国家サイバー統括室）
主査	デジタル庁統括官（デジタル社会共通機能担当）
	総務省サイバーセキュリティ統括官
	経済産業省商務情報政策局長
構成員	内閣官房内閣審議官（内閣官房副長官補付）
	内閣府科学技術・イノベーション推進事務局統括官
	警察庁長官官房技術総括審議官
	デジタル庁統括官（戦略・組織担当）
	外務省大臣官房サイバーセキュリティ・情報化参事官
	文部科学省研究振興局長
	経済産業省イノベーション・環境局長
	防衛省大臣安房サイバーセキュリティ・情報化審議官

※会議は非公開（議事要旨及び配付資料は原則公開）

＜スケジュール＞

令和7年6月30日	令和7年7～11月	令和7年11月頃	令和8年度中
第1回関係府省庁連絡会議 〇検討開始	〇課長級会合による検討	第2回関係府省庁連絡会議 〇工程表(ロードマップ)の骨子	第3回関係府省庁連絡会議 〇工程表(ロードマップ)の策定

＜検討すべき論点＞

〇 量子計算機の開発・普及状況、危殆化する公開鍵暗号等の特定とその時期
〇 諸外国の動向の把握
〇 PQCの安全性等の評価・確認とその時期
〇 PQCへの移行期限及び危殆化した公開鍵暗号等の利用に係る停止の時期
〇 政府機関等の移行への対応に必要な支援策等
〇 政府機関等の移行にむけた工程表（ロードマップ）の策定　など

サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項
令和7年5月29日 サイバーセキュリティ戦略本部

量子技術については、その進展に伴い、現在広く使われている公開鍵暗号の危殆化が懸念されているところ。そのため、諸外国や暗号技術検討会（CRYPTREC）における検討状況を踏まえ、多岐にわたる課題に対応するための関係省庁による検討体制を立ち上げ、**政府機関等における耐量子計算機暗号（PQC）への移行の方向性について、次期サイバーセキュリティ戦略**に盛り込む。

https://www.cryptrec.go.jp/